Computers and Electrical Engineering 000 (2018) 1–16

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

New security approach in real-time wireless multimedia sensor networks☆

Amina Msolli*, Abdelhamid Helali, Hassen Maaref

Laboratory of Micro-Optoelectronic and Nanostructures, Faculty of Sciences, University of Monastir, Avenue de l"Environnement, Monastir 5000, Tunisia

ARTICLE INFO

Article history:
Received 26 December 2016
Revised 15 January 2018
Accepted 15 January 2018
Available online xxx

Keywords:
Wireless multimedia sensor network (WMSN)
Shift-AES
Image symmetric key encryption algorithm
Gray scale image
High definition image
Block cipher modes

ABSTRACT

Real time multimedia applications are increasingly achieving success in the everyday world. A diversity of applications has appeared in the wireless sensor network, where the energy consumption is a very important factor in wireless multimedia sensor networks (WMSN) to increase network lifetime. Thus, multimedia data transmission relies on safety to protect personal life. However, because of constraints, the standard encryption algorithms are not compatible with this domain. This article investigates a new approach called Shift-Advanced Encryption Standard (Shift-AES). This approach modifies the AES algorithm to make it compatible with WMSN. Experimental studies of the new approach maintain a better level of safety with a decrease in execution time of the Central Processing Unit. A comparison is made between the new approach and the algorithms in the existing literature.

1. Introduction

Wireless multimedia sensor network [1–3] is a new domain. It blends the wireless sensor network and multimedia applications. This network is realized by a number of sensor nodes loaded with micro-cameras. In a scope, a set of standard sensor nodes with micro-cameras is laid out in a random manner. These nodes are autonomous in their functioning. Each node allows to get, to collect and to pass on the data between them up to the sink. The sink aggregates the data then sends it by satellite or internet to the user as shown in Fig. 1.

Each sensor node is characterized by three units (capture, processing and transmission) and a battery. The use of battery makes the wireless sensor network a large domain of scientific research [4], with the aim of minimizing the energy consumption of the node, and consequently, increasing the lifetime of the network. The low cost of sensor nodes is a second factor that allows the evolution of the search domain or the diversity of the applications. There exist civil, medical and military applications.

The material constraints of the sensor network and the hostile environment of the applications in several problems to be resolved. One of the problems of wireless multimedia sensor network is the security of data to be transmitted in order to protect it against attacks. Hence the dependence on a new encryption algorithm to meet the challenge. Today, several encryption algorithms have been proposed in the literature, such as DES [5,6], 3DES [5], Blowfish [7] IDES [8], RC6 [9], TEA [10] SEA [11] and AES [12,13]. These various algorithms are operated with scalar data or text, and rarely to use for

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. V. Sai.

* Corresponding author.
E-mail addresses: amina.msolli@gmail.com (A. Msolli), Abdelhamid.Helali@isimm.rnu.tn (A. Helali).

https://doi.org/10.1016/j.compeleceng.2018.01.016
0045-7906/© 2018 Published by Elsevier Ltd.

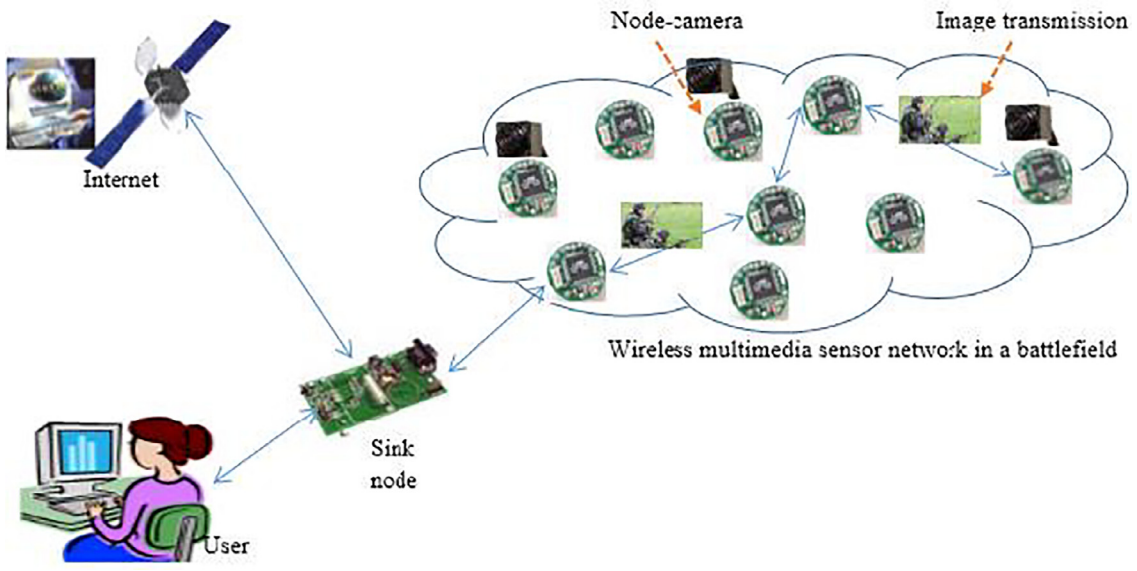

Fig. 1. Wireless multimedia sensor network in a battlefield.

the multimedia data [14]. Because the multimedia data admit a large volume and redundancy and a need of real-time interaction.

Among the purposes, energy consumption is a very important factor in wireless multimedia sensor network (WMSN) to increase network lifetime. So, multimedia data transmission depends on safety to protect personal life [15]. Because of physical constraints and the hostile environment, the standard encryption algorithms are not compatible with this domain. This article investigates a new approach called Shift-AES. This approach modifies the AES algorithm to make it compatible with WMSN. The modification consists in replacing the Mix-Columns transformation of the AES algorithm by another Shift-Columns transformation, which maintains the same principle of Shannon and reduces enormously the energy consumption. In addition, a second modification causes the rearrangement of the transformations in the proposed algorithm design. This change improves the entropy and the execution time. Experimental studies of the new approach indicate a better level of safety with a decrease in execution time of the Central Processing Unit (CPU). A comparison is made between the new approach and the algorithms in use in the literature.

The paper is organized as follows: it starts with a literature review. Subsequently, it explains the new Shift-AES approach. Then, it is followed by a discussion of the performance of the experimental results. And it finishes with a conclusion.

2. Related works

During these last years, several investigations have been undertaken into encryption algorithms, with the purpose of improving existing algorithms according to the needs of different applications. In this article, we are specifically interested in symmetric encryption algorithms by block. Some works in the literature are mentioned below.

First of all, a study on the initial AES algorithm is outlined briefly. AES (Advanced Encryption Standard) [12,13] is a symmetric encryption standard by block. It replaces the old Data Encryption Standard (DES). It is based on a matrix named State of 4×4 bytes. The AES algorithm consists of three main parts. In the encryption phase, the entry undergoes various transformations known as Sub Bytes, Shift Rows, Mix Columns and Add Round Key. These processes run with a routine called round proportional to key size. Thus, the decryption phase is similar to that of encryption except that all transformations are inverted. Then, finally a third part joins the two phases: which is the keys expansion. The AES algorithm takes the secret key and performs a key expansion routine to generate a key schedule.

The AES algorithm makes it possible to use keys of various sizes, like 128, 192 and 256 bits to encrypt and decrypt data in blocks operating on 128 bits. The choice of key size is similar to the number of rounds: 10, 12 and 14 respectively.

Shtewi et al. [16] and Kamali et al. [17] tried to modify the AES algorithm to apply it to the real-time multimedia data and to minimize execution time. The authors realized an adjustment to the ShiftRow process. The modification was made in two phases depending on the value of the first cell of the state. If the first number of the state was even or odd, then a certain number of different offsets was made on the various lines of the state.

In the same order, Wadi and Zainal [18,19] proposed another modification concerning the initial AES algorithm. Three changes were introduced to reduce the cost of calculations and to increase the level of safety. The first modification was based on the decrease of the number of rounds of the transformation MixColumn down to five rounds, which allows a decrease in the encryption time. A second modification is the replacement of the S-box by another one that is simpler

Please cite this article as: A. Msolli et al., New security approach in real-time wireless multimedia sensor networks, Computers and Electrical Engineering (2018), https://doi.org/10.1016/j.compeleceng.2018.01.016